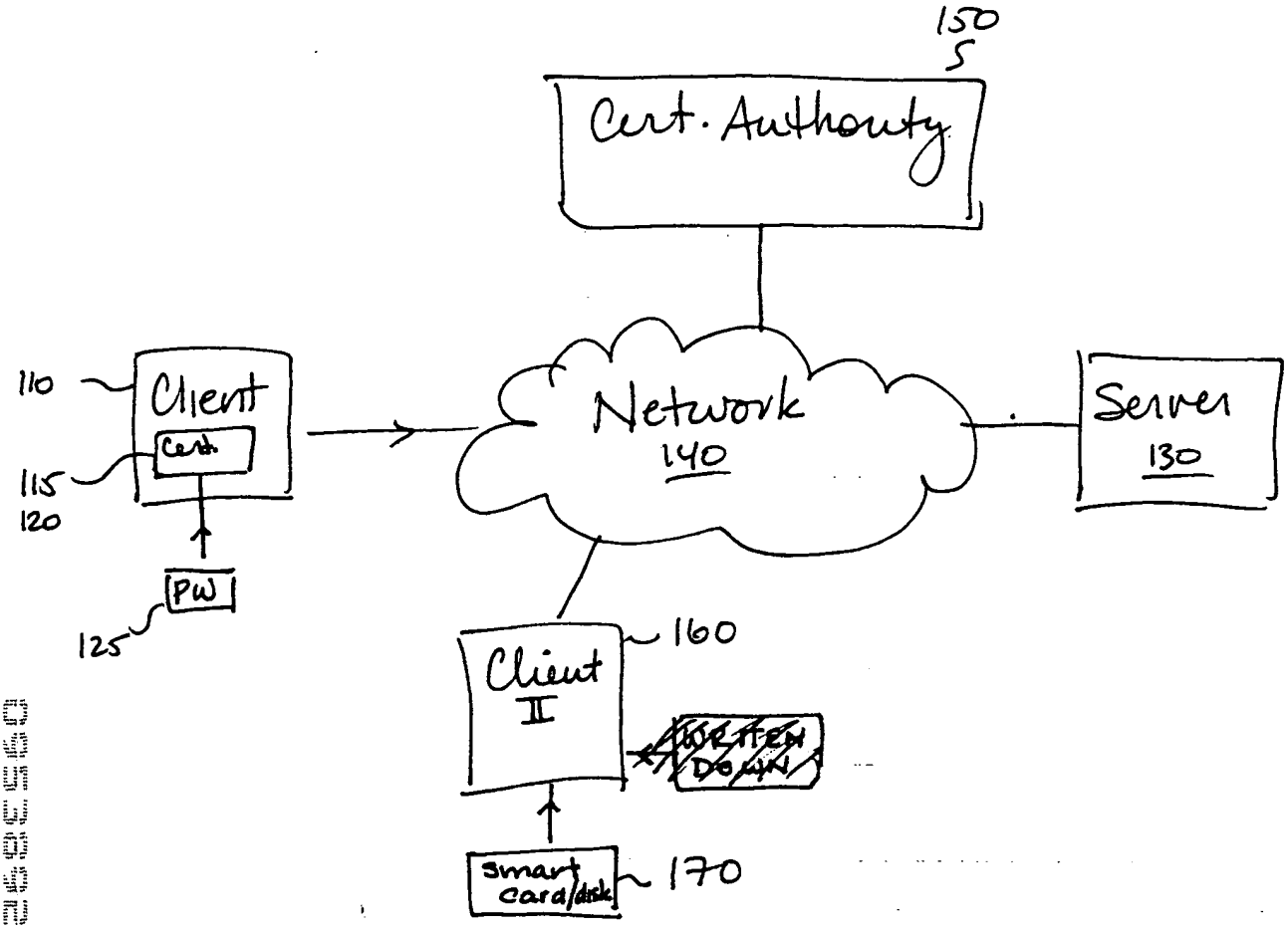


FIG 1
(Prior Art)

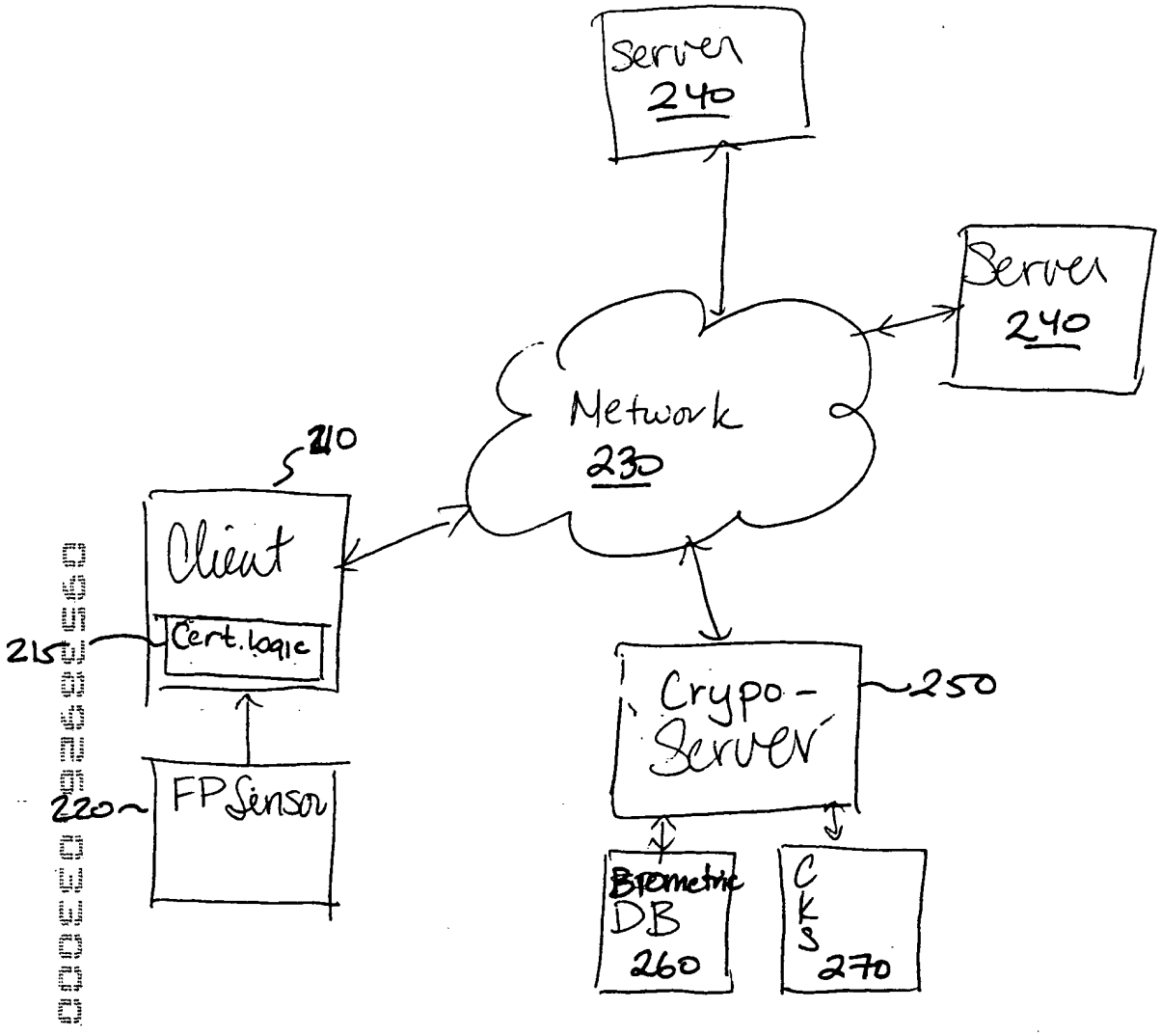

Server
240
Server
240
Network
230
210
Client
Cert. logic
215
220
FP Sensor
Crypo-
Server
250
Biometric
DB
260
C
K
S
270

FIG. 2

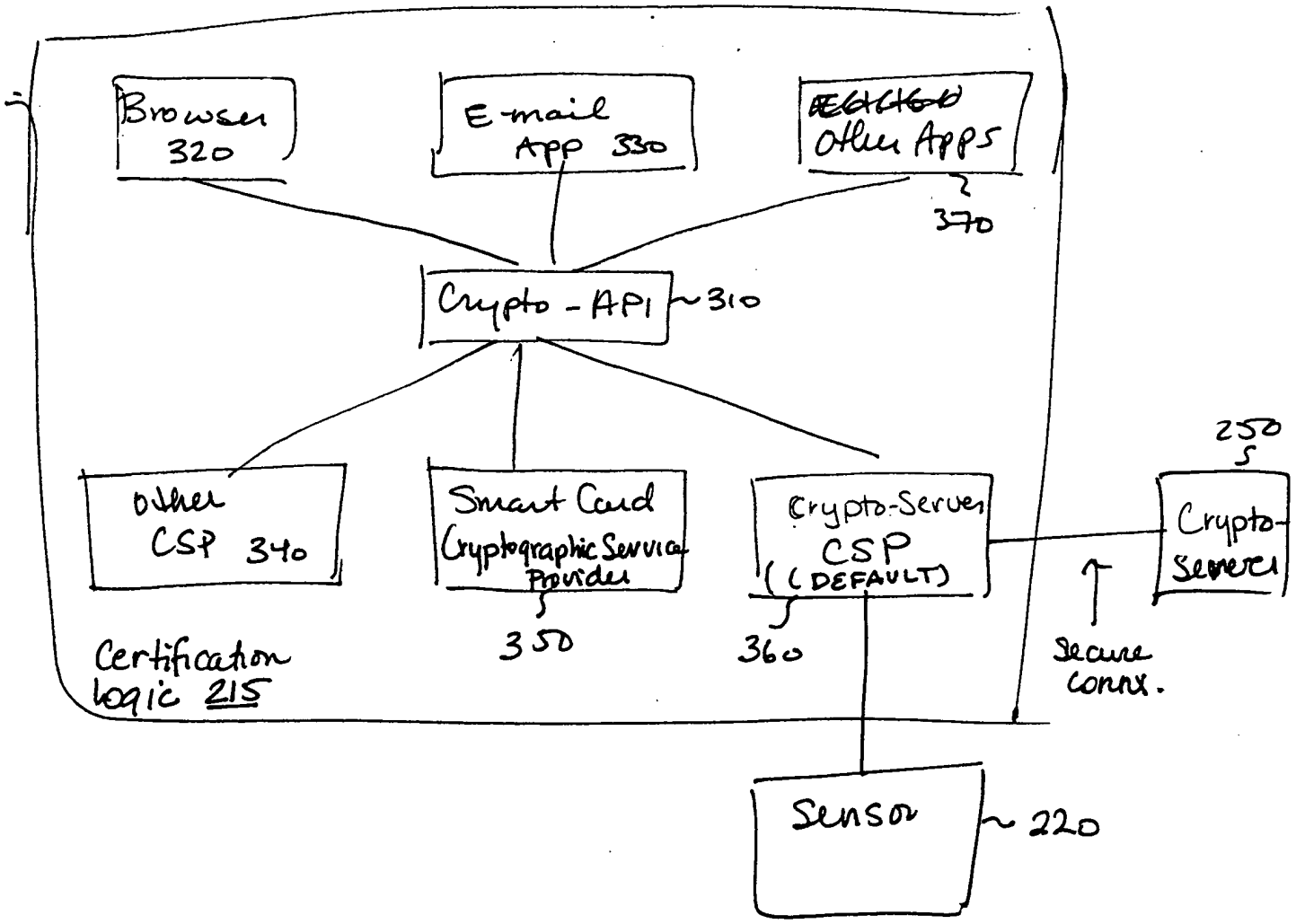
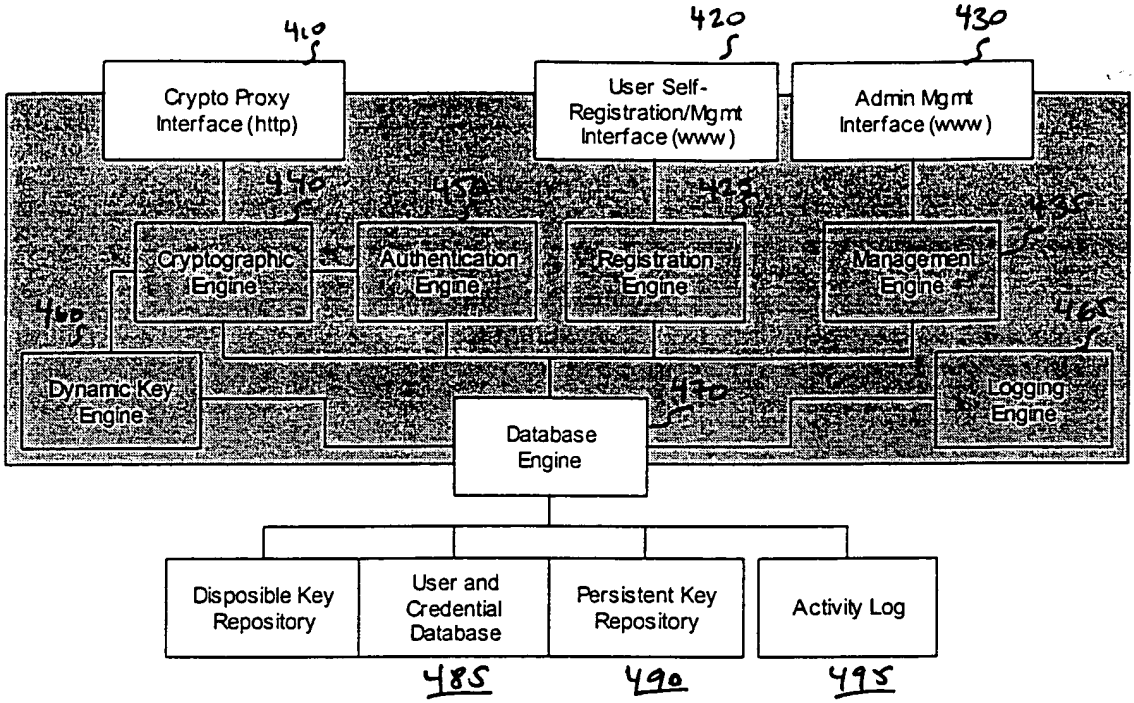


FIG. 3

Block Diag of Comp. Sys.



Crypto-Server 250

FIG. 4

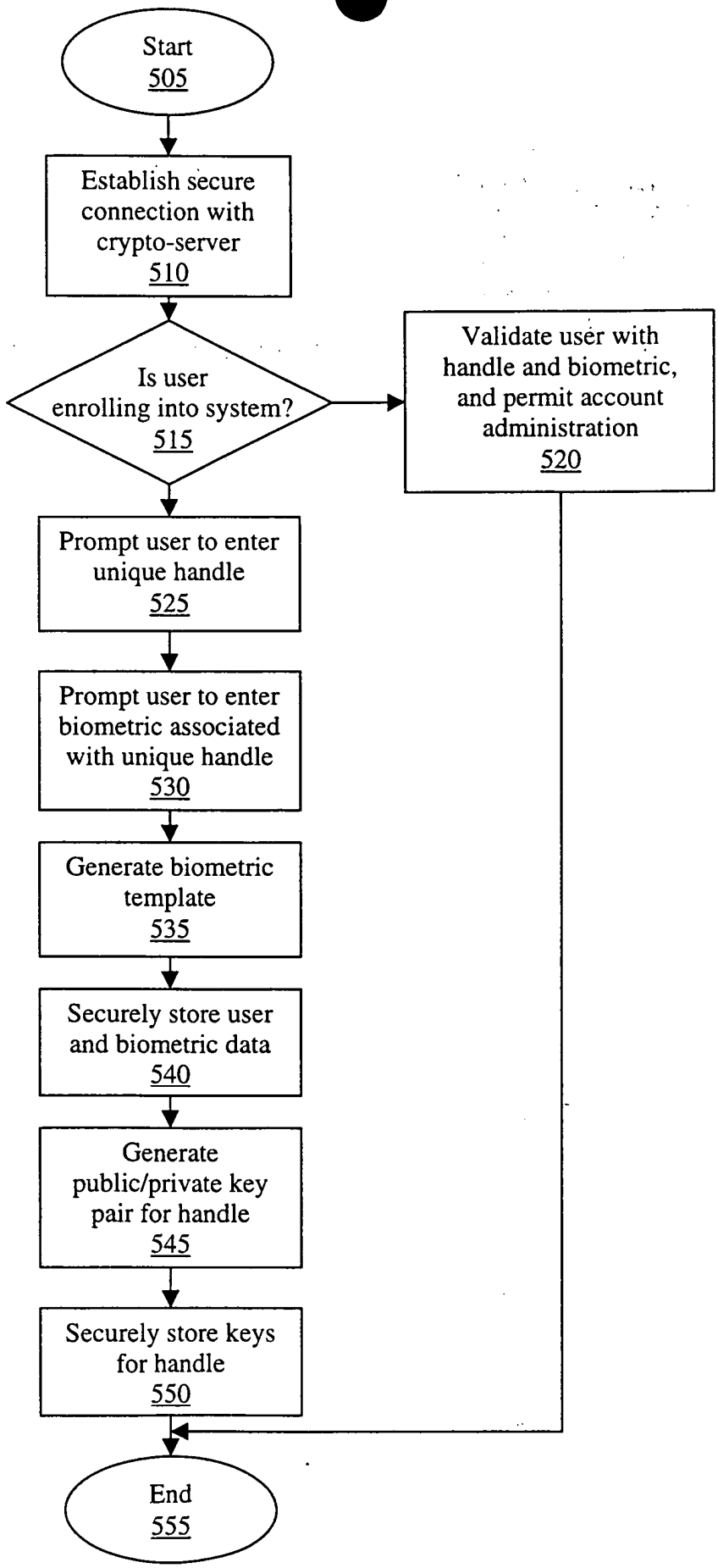
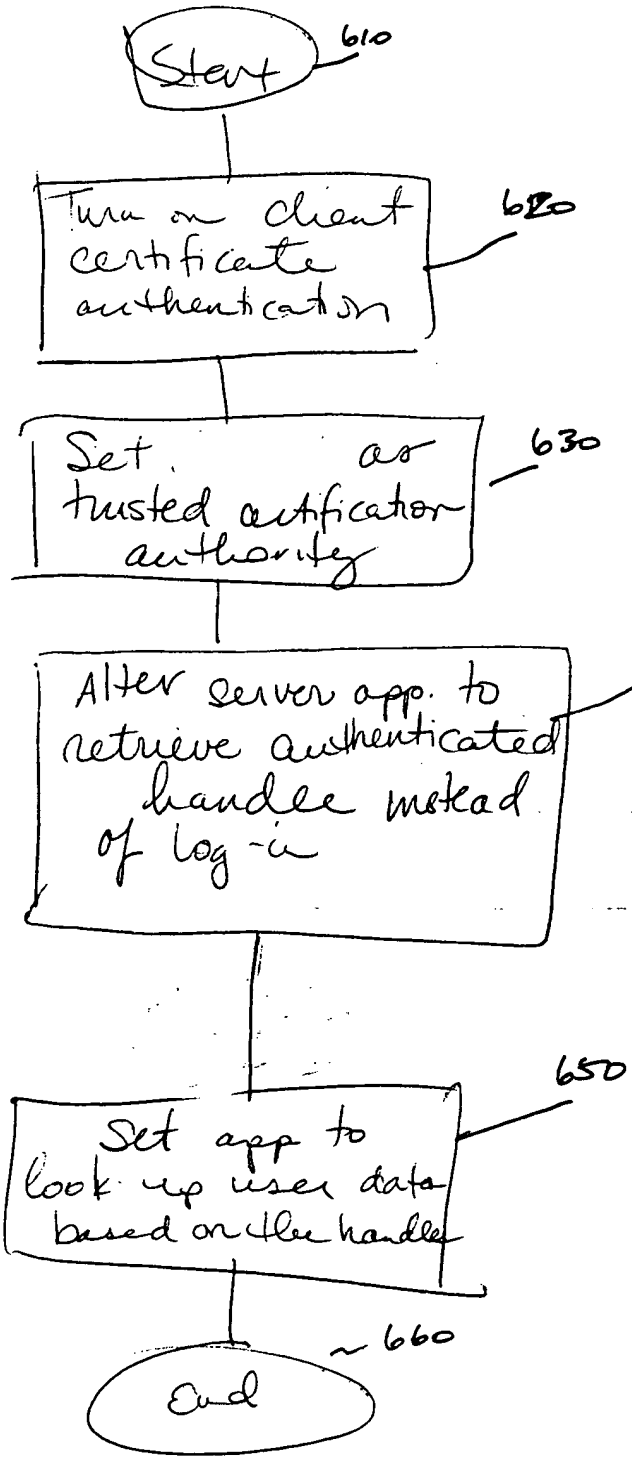

Start
505
Establish secure connection with crypto-server
510
Is user enrolling into system?
515
Validate user with handle and biometric, and permit account administration
520
Prompt user to enter unique handle
525
Prompt user to enter biometric associated with unique handle
530
Generate biometric template
535
Securely store user and biometric data
540
Generate public/private key pair for handle
545
Securely store keys for handle
550
End
555

Fig. 5



(Readying Server to Accept BioCert)

FIG. 6

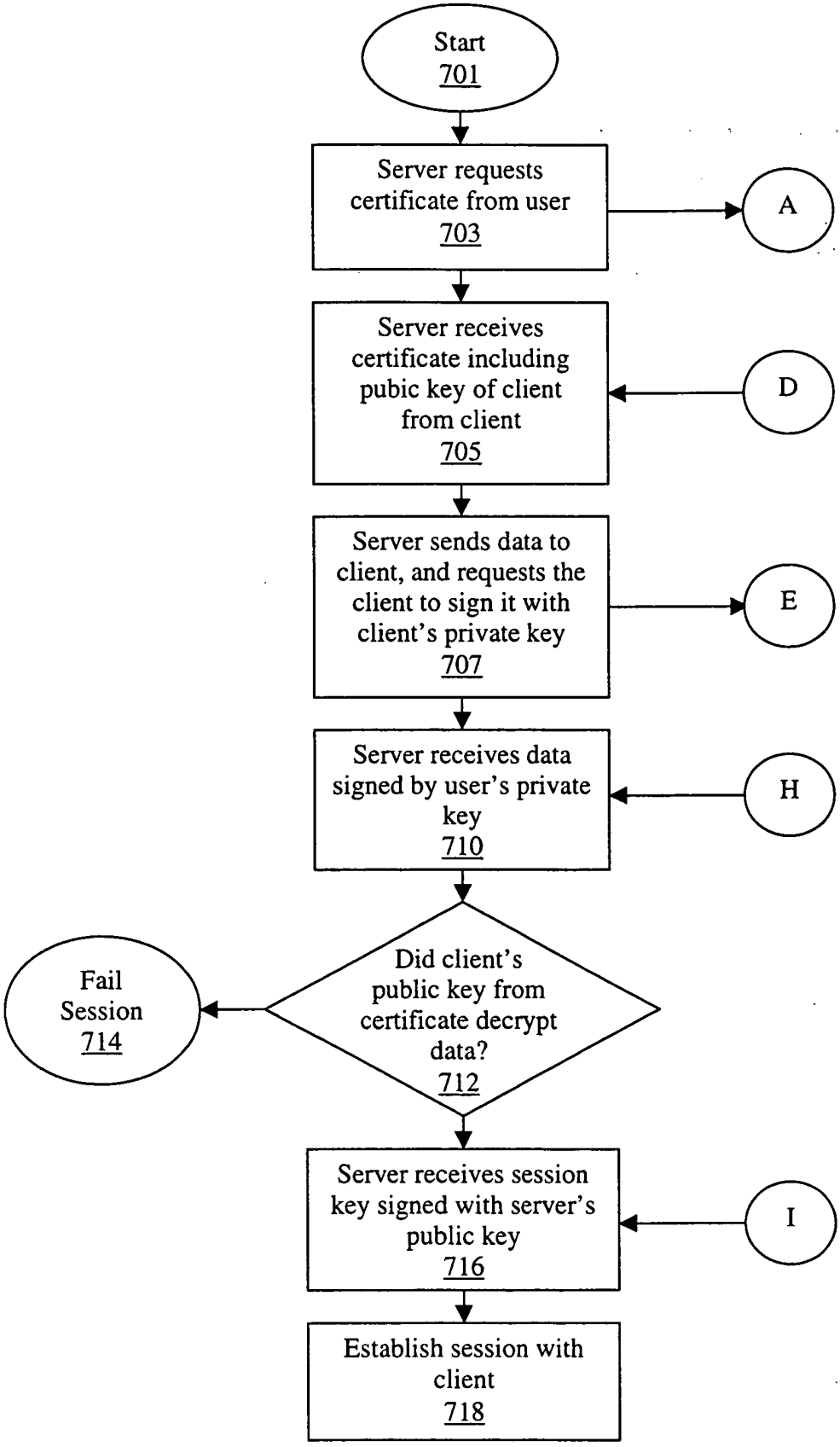

Start
701
Server requests certificate from user
703
A
Server receives certificate including pubic key of client from client
705
D
Server sends data to client, and requests the client to sign it with client's private key
707
E
Server receives data signed by user's private key
710
H
Did client's public key from certificate decrypt data?
712
Fail Session
714
Server receives session key signed with server's public key
716
I
Establish session with client
718

Fig. 7A

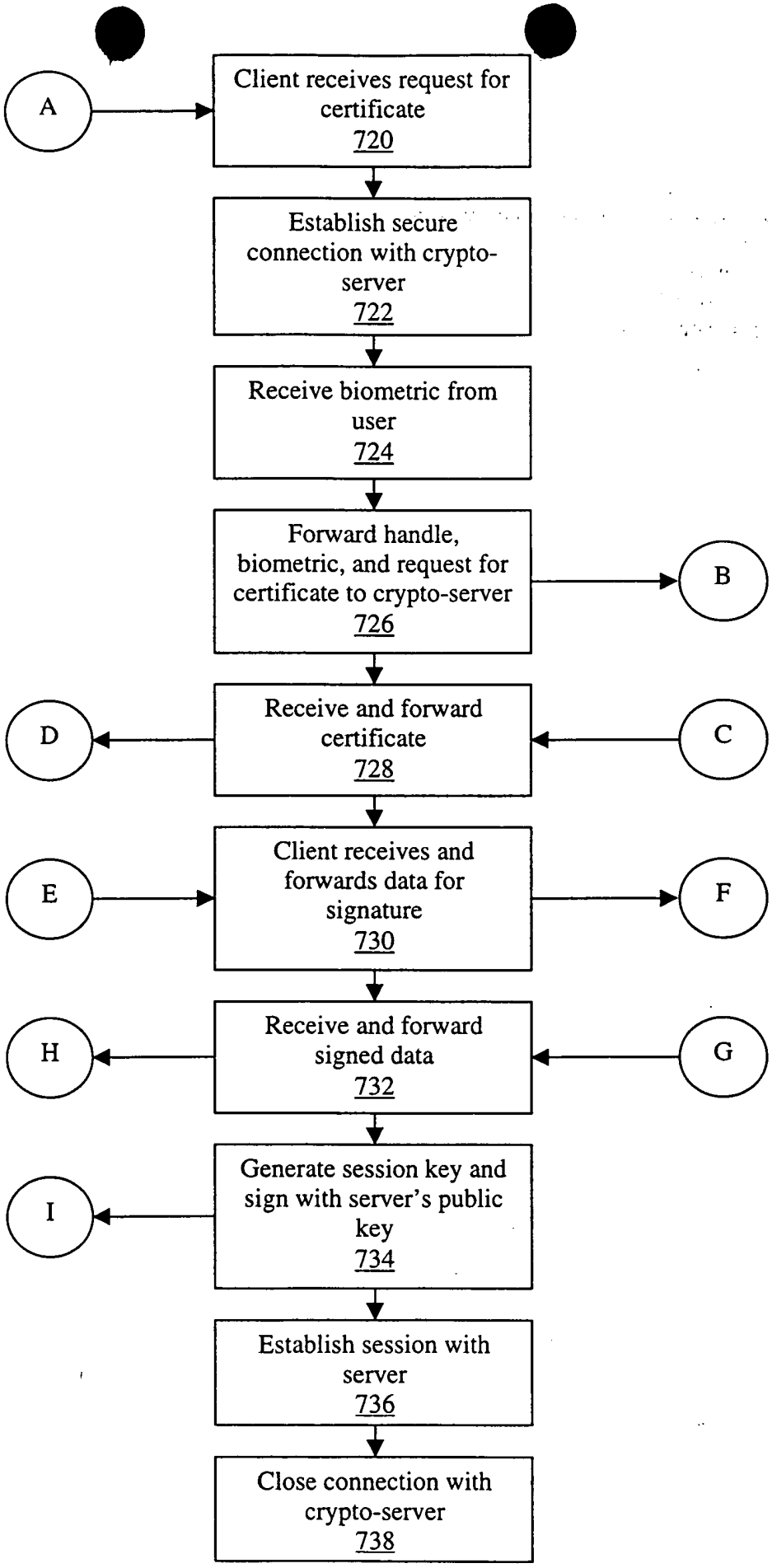

A
Client receives request for certificate
720
Establish secure connection with crypto-server
722
Receive biometric from user
724
Forward handle, biometric, and request for certificate to crypto-server
726
B
D
Receive and forward certificate
728
C
E
Client receives and forwards data for signature
730
F
H
Receive and forward signed data
732
G
I
Generate session key and sign with server's public key
734
Establish session with server
736
Close connection with crypto-server
738

Fig. 7B

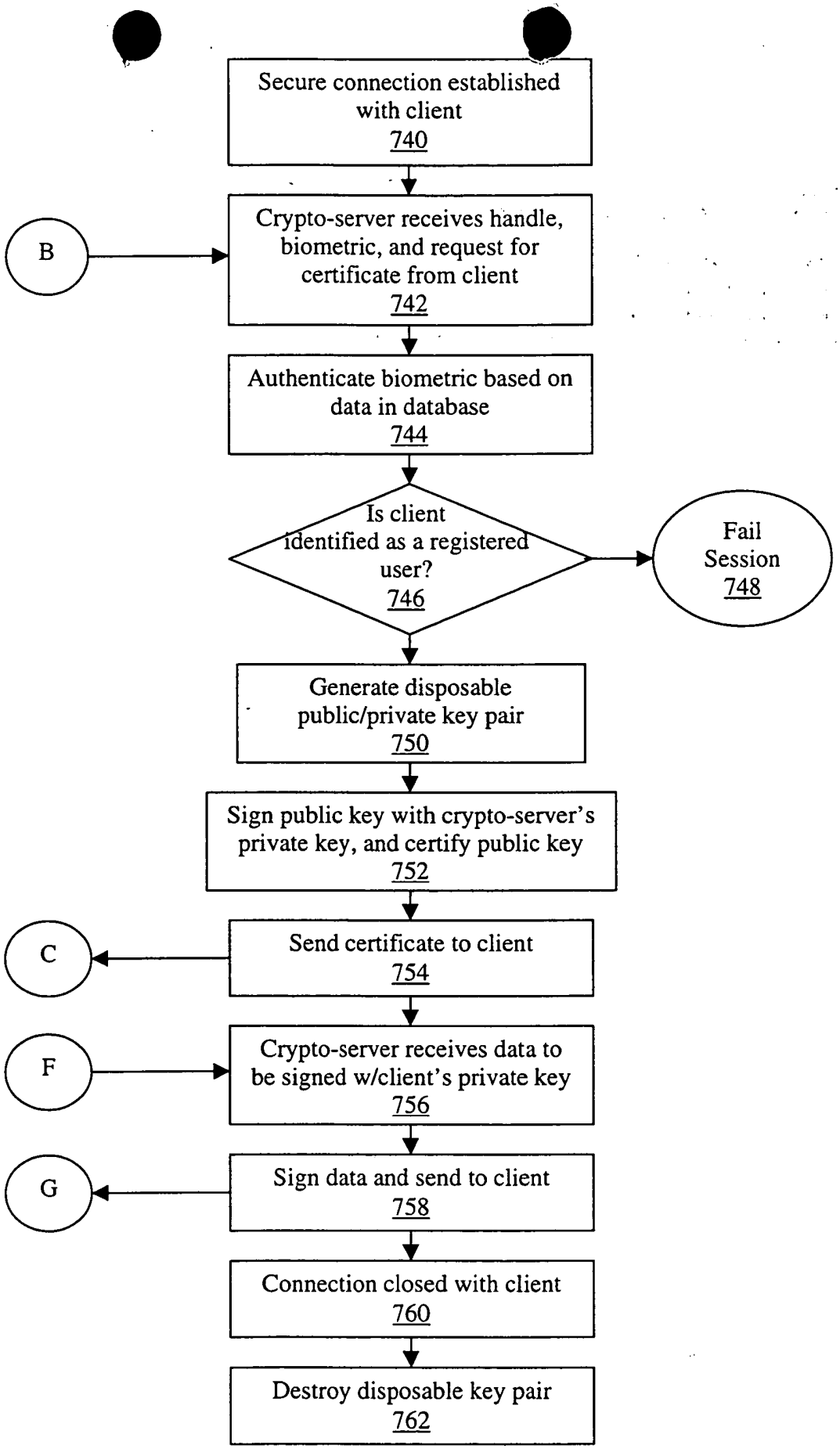

Secure connection established with client 740
B
Crypto-server receives handle, biometric, and request for certificate from client 742
Authenticate biometric based on data in database 744
Is client identified as a registered user? 746
Fail Session 748
Generate disposable public/private key pair 750
Sign public key with crypto-server's private key, and certify public key 752
C
Send certificate to client 754
F
Crypto-server receives data to be signed w/client's private key 756
G
Sign data and send to client 758
Connection closed with client 760
Destroy disposable key pair 762

Fig. 7C

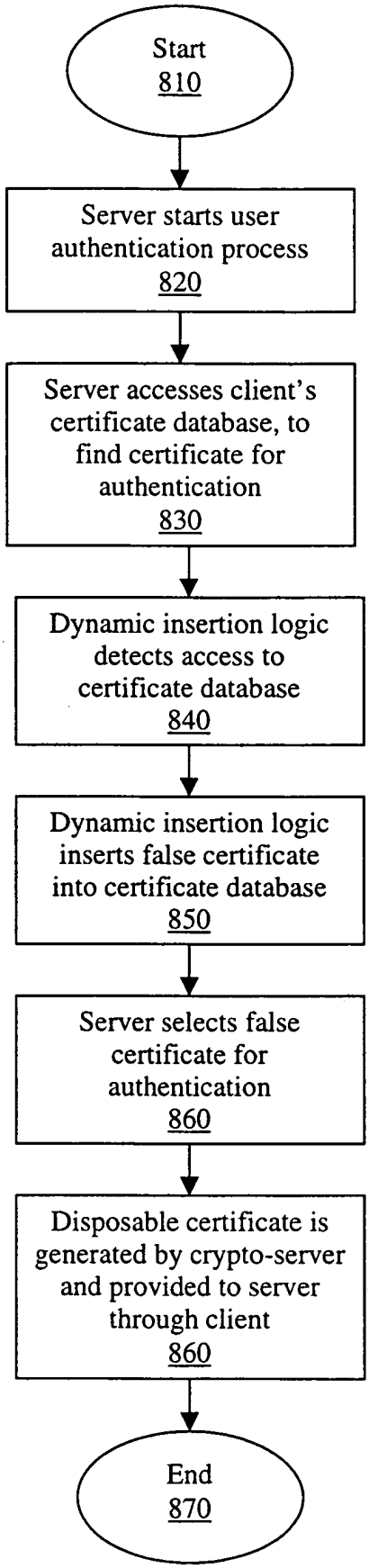

Start
810
Server starts user authentication process
820
Server accesses client's certificate database, to find certificate for authentication
830
Dynamic insertion logic detects access to certificate database
840
Dynamic insertion logic inserts false certificate into certificate database
850
Server selects false certificate for authentication
860
Disposable certificate is generated by crypto-server and provided to server through client
860
End
870

Fig. 8

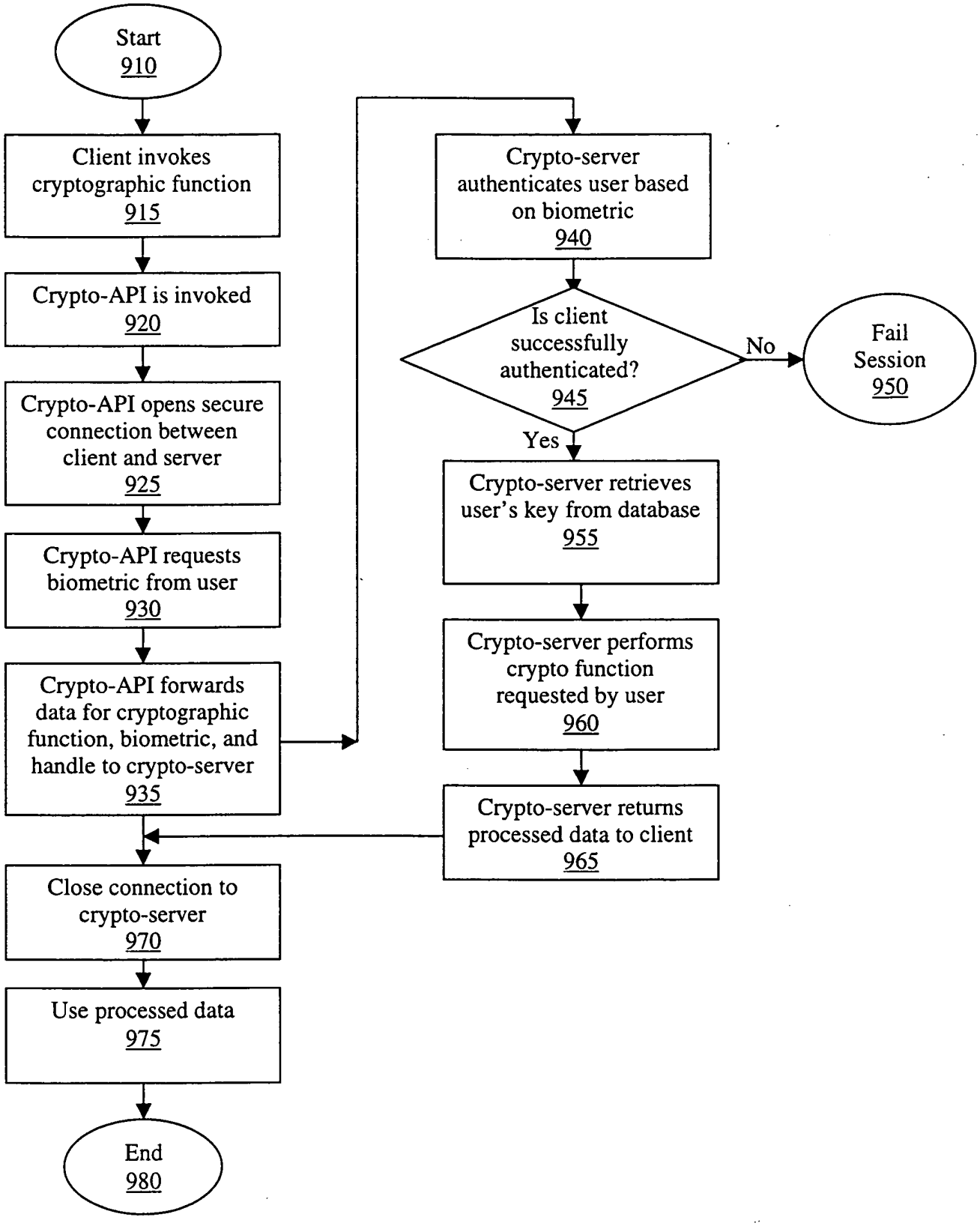

Start
910
Client invokes cryptographic function
915
Crypto-API is invoked
920
Crypto-API opens secure connection between client and server
925
Crypto-API requests biometric from user
930
Crypto-API forwards data for cryptographic function, biometric, and handle to crypto-server
935
Close connection to crypto-server
970
Use processed data
975
End
980
Crypto-server authenticates user based on biometric
940
Is client successfully authenticated?
945
No
Fail Session
950
Yes
Crypto-server retrieves user's key from database
955
Crypto-server performs crypto function requested by user
960
Crypto-server returns processed data to client
965

Fig. 9

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.